USAWC STRATEGY RESEARCH PROJECT

Information Operations: Reassessing Doctrine and Organization

by

LTC Randall L. Mackey
US Army

COL Felix Castro
Project Advisor

The views expressed in this academic research paper are those of the author and do not necessarily reflect the official policy or position of the U.S. Government, the Department of Defense, or any of its agencies.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY) 07-04-2003	2. REPORT TYPE	3. DATES COVERED (FROM - TO) xx-xx-2002 to xx-xx-2003

4. TITLE AND SUBTITLE
Information Operations: Reassessing Doctrine and Organization
Unclassified

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Mackey, Randall L. ; Author

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME AND ADDRESS
U.S. Army War College
Carlisle Barracks
Carlisle, PA17013-5050

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS
,

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APUBLIC RELEASE
,

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached file.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:

a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified

17. LIMITATION OF ABSTRACT
Same as Report (SAR)

18. NUMBER OF PAGES
41

19. NAME OF RESPONSIBLE PERSON
Rife, Dave
RifeD@awc.carlisle.army.mil

19b. TELEPHONE NUMBER
International Area Code
Area Code Telephone Number
DSN

ABSTRACT

AUTHOR: LTC Randall L. Mackey

TITLE: Information Operations: Reassessing Doctrine and Organization

FORMAT: Strategy Research Project

DATE: 17 March 2003 PAGES: 41 CLASSIFICATION: Unclassified

Information operations will play a key role in pursuing information superiority as part of the Joint Vision 2020 goal of achieving full spectrum dominance. Despite the importance of information operations within the U.S. vision of future conflict, the U.S. military does not have a consistent and coherent understanding of information operations. Information operations mission areas are ill defined and what should be basic terminology is complex, full of nuances, and inconsistent. Organization within DoD to accomplish IO missions is also less than optimal. In some cases different unrelated IO missions are assigned to organizations in an effort to consolidate responsibility for IO. Yet in other instances closely related missions that should be centralized are assigned to different organizations. This paper examines the various mission areas under IO as currently defined, proposes modifications, and presents a new taxonomy for IO and IO component mission areas. This paper also examines current IO organizations within DoD and makes recommendations for realignment of IO missions.

TABLE OF CONTENTS

INFORMATION OPERATIONS MISSION AREAS AND ORGANIZATION: AN ASSESSMENT

Nothing in cyberspace is new.

— Bruce Schneier, *Secrets and Lies: Digital Security in a Networked World*

Joint Vision 2020 (JV 2020) identifies information superiority as one of two key enablers of the transformation of U.S. joint force capabilities. Under JV 2020 U.S. forces will leverage information superiority while employing the primary operational concepts of dominant maneuver, precision engagement, focused logistics, and full dimensional protection in pursuit of full spectrum dominance over potential adversaries.[1] Since the U.S. would employ information operations (IO) as a primary means to gain information superiority JV 2020 identifies IO as "essential to achieving full spectrum dominance."[2] Although IO is an important part of how the U.S. will fight future conflicts, the understanding of IO within the U.S. military is immature and inconsistent. As currently defined, IO is a broad area with many diverse subcomponents. The wide array of missions within IO, along with the inability to shed past notions of IO, hinder the U.S. military in implementing IO in a more effective, coherent, and consistent manner.

Similarly the U.S. military organization for executing IO is fractured and not optimal. In some cases within DoD, responsibility for closely related areas is not consolidated. Conversely, in other instances responsibilities for disparate functions have been unified under single organizations. The result has been limited effectiveness in executing well-planned and coordinated information operations in support of larger objectives, along with overly difficult and complicated efforts to protect our own information, information systems, and networks. These organizational limitations may spring from our understanding of IO and how the components of IO relate to one another.

The dangers, risks, and threats to DoD systems have been widely publicized and reported. Although I think the risks are not in general well understood and have been overstated in some areas, I will not address those risks. I will examine current IO doctrine and definitions and make recommendations for redefining certain aspects of IO and realigning the subcomponents of IO under a new taxonomy. I will also examine the current organization of DoD regarding IO and make recommendations for realigning IO missions and functions. Through more consistent IO doctrine and streamlined IO organization, DoD can improve its ability to protect our own information assets and to effectively employ IO against our adversaries.

INFORMATION OPERATIONS DEFINITION AND DOCTRINE

Joint Publication 3-13 (JP 3-13), *Joint Doctrine for Information Operations,* defines IO as "actions taken to affect adversary information and information systems, while defending one's own information and information systems."[3] This basic definition of IO is simple and clear, but the implications of this definition are many and diverse. IO is complex because it not only concerns information, but the systems that convey that information, and the use of inaccurate information to influence an adversary as well.

Information is the very basis of any country's national will or of any organization's unity (although those in power may have distorted information to gain and hold power). Military forces depend on information to be able to execute even the simplest maneuver or operation. Leaders at all levels rely on information to make decisions. Some areas of IO are concerned with what an opponent can be made to believe is true vice what is actually true. Inaccurate information, or information of which the accuracy is in doubt, could cause an adversary to make a bad decision or prevent an adversary from making necessary decisions. Information operations in the form of protecting one's own information while intercepting, interrupting, or distorting an enemy's information is nearly as old as warfare itself.

Information systems support the gathering, processing, storing, and dissemination of information. Information systems that rely upon computers and electro-optical communications permeate the developed world. Computer-based information systems are in wide use within our military forces to perform tasks from as simple as enabling person-to-person communications to as complex as the automated relay of target data to weapons systems in order to guide "smart" munitions to precise targets. Information systems are increasingly found in the developing parts of the world and within evolving militaries that hope to use technology to gain an edge over their adversaries. The technology that enables the collection, processing, and transmission of information can create vulnerabilities and it is these vulnerabilities that are the basis of certain aspects of information operations that have more recently emerged.

Information operations are an important focus of the U.S. military. The U.S. military has translated this focus into organizations, resources, policy, and doctrine focused on the various aspects of IO. Even with this focus, it is not clear that IO is well understood within the U.S. military or that we are properly organized or directing resources to achieve the purposes we intend to achieve via IO. Regarding the defense of our own information and associated systems, numerous writers and experts have pointed out our increasing reliance on information technology. This reliance may not only be giving us an edge over potential adversaries, but may also be creating an Achilles heel in the form of vulnerabilities that our adversaries may not likewise share. Effective defensive IO is critical to protecting U.S. capabilities across the spectrum of conflict. Regarding the use of offensive IO, the U.S. seems hindered in employing coordinated IO efforts to achieve desired effects on adversaries. It is imperative that the U.S. military come to a well developed, consistent, and coherent understanding of IO and then apply associated resources in the most effective manner possible.

JV 2020 lays out achieving *full spectrum dominance* over adversaries as the primary goal of our joint forces. After full spectrum dominance, the second concept explained in JV 2020 is *information superiority*. Joint Publication1-02 (JP1-02), the *Dictionary of Military and Associated Terms*, defines information superiority as "that degree of dominance in the information domain which permits the conduct of operations without effective opposition."[4] The conditions described in this definition may not in fact be sufficient to warrant a declaration of information superiority. Unlike a more classic definition of superiority, that of *air superiority*, JP 3-13 does not express superiority in the information realm in terms of a degree of capability relative to an adversary or in terms of supporting land, air, and sea operations. Other publications also dilute the concept of information superiority. JV 2020 explains that in noncombat or ambiguous situations information superiority is achieved when "friendly forces have the information to achieve operational objectives."[5] It is not immediately clear why this particular clarification is included in JV 2020, but this illogical and apparently needless conclusion highlights an incomplete understanding of our goals in the information realm. Despite these shortcomings with the current understanding of what constitutes information superiority, in conflict the U.S. would conduct IO, in support of maneuver warfare and other types of operations, and seek to achieve an information advantage over adversaries in order to achieve success.

JP 3-13 also includes a discussion of *information warfare*. JP 3-13 defines information warfare (IW) as "IO conducted during time of crisis or conflict (including war) to achieve or promote specific objectives over a specific adversary or adversaries."[6] It is not clear that we need two different terms, one for peacetime and one for wartime, to describe the same type of operations. Most likely the intent was to allow for the conduct of IO under conditions other than war and to justify not having those actions interpreted as acts of war. This is only one example of how the IO arena is replete with terminology that is redundant and ambiguous.

U.S. doctrinal limitations concerning IO can be traced to a number of factors. U.S. IO doctrine groups a diverse array of mission areas under the single term *IO*. This leads to unnecessary centralization and less than optimal groupings of IO missions under certain organizations. Through an assessment of current IO doctrine and the relationships of the various mission areas of IO, the U.S. military can come to a better understanding of IO and allocate resources more effectively.

CURRENT INFORMATION OPERATIONS MISSION AREAS

COMPONENT AREAS OF INFORMATION OPERATIONS

What DoD lacks in the form of published offensive IO capability or in the form of protection for widely publicized vulnerabilities is contrasted by the existence of a plethora of terminology. This terminology is often complex, confusing, incomplete, or ambiguous and in some cases different publications offer contradictory information pertaining to IO terminology and mission areas. Differences also exist between the doctrine and terminology of the Services, and between that of the Services and the Joint environment. JP 3-13 divides IO into three basic mission areas: *offensive, defensive, and IO-related activities*.[7] A short explanation of each of the areas and their specific related missions serves to provide a framework for analyzing U.S. IO doctrine.

Offensive Information Operations

JP 3-13 states that *offensive information operations* include electronic warfare, psychological operations, physical attack/destruction, operations security, deception, and special information operations. JP 3-13 also states that offensive IO are not limited to these categories and that offensive IO "could include" computer network attack.[8] That computer network attack is not considered a primary component of offensive information operations seems unusual and perhaps this will be changed in later updates. It is important to understand the definitions and doctrine associated with each component area of offensive IO and a short discussion of each area follows.

ELECTRONIC WARFARE

JP 3-13 defines electronic warfare (EW) as "any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy."[9] What sets EW apart from other areas of IO like computer network attack is that EW relies on electromagnetic transmissions rather than other means of access in order to achieve effects. Perhaps more simply restated, offensive EW entails the transmission of radio frequency waves to achieve desired effects. The offensive aspects of EW include jamming, electromagnetic deception, and the use of electromagnetic pulse (EMP) to destroy or degrade enemy electronic equipment. In the past EMP was usually considered a byproduct of nuclear detonations, but there has been more recent interest in the use of EMP generated by other means including vehicle-mounted devices and even microwave generators carried on cruise missiles.[10] Notably absent from the existing Joint definition of offensive EW is interception and exploitation of enemy electromagnetic transmissions. This is a recurring observation throughout current IO terminology--interception and exploitation are not currently included as aspects of IO.

PSYCHOLOGICAL OPERATIONS

Psychological operations (PSYOP) are "planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals."[11] Key in this definition is the limitation to "foreign audiences." Military employment of PSYOP against domestic audiences is illegal. Additionally any use of PSYOP against allied audiences would be inappropriate. Increasingly the term *perception management* is gaining popularity within DoD. Perception management is not an equivalent term for PSYOP as perception management includes not only PSYOP but also aspects of operations security and deception. Perception management also includes the concept of *truth projection*--emphasizing factual information to influence certain audiences (as opposed to deceiving these audiences).[12] Selective truth projection intended for domestic or allied consumption causes concerns similar to those associated with employing PSYOP in similar circumstances.

PHYSICAL ATTACK/DESTRUCTION

Physical attack or destruction is the most basic form of IO. Physical attacks could be directed at enemy command and control or communications assets or could be directed at enemy assets attempting to jam, intercept, or otherwise affect friendly communications, command and control, or other information assets. Nodes where communications paths merge or sites where centralized data processing occurs offer particularly lucrative targets. Some suggest that physical attack should not be included as an element of IO and that IO should be limited to those means that employ only electromagnetic or computer network attack methods.[13] This argument bears little merit as physical attack may in fact attain IO goals better than some form of "soft" attack. As one influential writer notes, "Blowing up a computer center is much better than exploiting a Windows 2000 vulnerability."[14] Including physical attack as an element of IO should also facilitate coordination, synchronization, and deconfliction of physical attack with other forms of IO. When we gain significant knowledge of an enemy asset we should always consider many factors and options. Do we attack, how do we attack, when do we attack, do we exploit to gain intelligence, or do we use the asset as a channel to deceive or employ PSYOP? We should make a conscious decision on which approach to take based on available intelligence, desired effects, and probability of success. It is important to consider all options and not to destroy something that could have been attacked or exploited to greater advantage by other means. In order to ensure the consideration of all options and to deconflict physical attack with other IO activities, it is essential to continue to consider physical attack/destruction as an element of IO.

COMPUTER NETWORK ATTACK

Computer network attack (CNA) includes "operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves." [15] Joint doctrine specifically excludes electronic attack (jamming, electromagnetic pulse) from CNA and limits the definition of CNA to methods that "[rely] on the data stream to execute the attack."[16] Computer network attack is what most have come to know as *hacking*—implanting or disseminating computer viruses or disrupting the operation of computers via the networks on which they rely for communications. Joint Publication 3-51 (JP 3-51) *Joint Doctrine for Electronic Warfare* includes the umbrella term *computer network warfare* [17] for the combination of CNA and computer network defense. Although other Joint publications separate EW from CNA, JP 3-51 includes a short discussion of the relationship between EW and CNA and suggests that EW is in fact a means to conduct "successful computer system penetrations."[18]

Other related terms in current usage within DoD are *computer network operations (CNO)* and *computer network exploitation (CNE).* U.S. Space Command (USSPACECOM) coined CNO as an umbrella term for the combination of CNA and computer network defense.[19] One should note that *computer network operations* is very different from *operating computer networks*, the latter being comprised of the activities to administer, operate, and maintain networks. CNE includes activities to penetrate or monitor computer networks for the purpose of gathering intelligence. Joint doctrine does not clearly include CNE as an element of CNO mirroring the exclusion of other forms of exploitation from IO. Again to highlight the profusion of terminology, Joint doctrine includes the terms computer network attack, computer network warfare, computer network operations, and computer network exploitation—all related terms but each with its own slightly different definition.

SPECIAL INFORMATION OPERATIONS

Special information operations (SIO) are not clearly defined in Joint publications and only described as "information operations that by their sensitive nature and due to their potential effect or impact, security requirements, or risk to the national security of the United States, require a special review and approval process."[20] Factors that may precipitate the elevation of particular IO to *special* status may be the intelligence sources and methods involved, possible strategic impacts, or basic operational security considerations. Some offensive IO methods may bear status as SIO if those methods might be limited to a single use. Once used, and if effective, potential adversaries would likely eliminate whatever vulnerabilities allowed that initial single use.

DECEPTION

Deception includes "those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce the enemy to react in a manner prejudicial to the enemy's interests."[21] Deception is considered both an offensive and a defensive IO measure as deception includes aspects of both modes of operation. Deception is intended to have an impact on an adversary (an offensive aspect), but deception normally conceals friendly intentions, dispositions, or capabilities (a defensive aspect). Deception includes physical means such as executing misleading troop maneuvers, and nonphysical means such as the transmission of false information or of misleading electronic signatures.

OPERATIONS SECURITY

Operational security (OPSEC) entails both a process to identify friendly information that may be helpful to an adversary and the measures taken to eliminate or reduce the adversary's ability to obtain or use that information.[22] As with deception, there are defensive and offensive aspects of OPSEC. Likewise there are physical and non-physical aspects of OPSEC such as preventing enemy visual observation of troop dispositions (a physical aspect) and preventing enemy interception of friendly communications (a nonphysical aspect).

Defensive Information Operations

JP 3-13 defines defensive IO as including information assurance, OPSEC, physical security, counterdeception, counterpropaganda, counterintelligence, EW, and SIO. As with offensive IO, it is important to understand the definitions and doctrine associated with each component area of defensive IO.

INFORMATION ASSURANCE

The five component areas of information assurance (IA) are availability, integrity, authentication, confidentiality, and nonrepudiation.[23] *Availability* simply means that a particular system or capability is available to support its intended purpose. *Integrity* implies that data contained within a system is accurate and unaltered. *Confidentiality* means that data is not accessible to those who should not have access. Authentication relies upon measures in place to verify identities before access is granted. Nonrepudiation means that the source of messages or other information is clear and cannot be questioned. In its broadest definition, the availability component of IA also includes protection, detection, and reaction capabilities.[24] Over time the term IA has increasingly come to be considered as only those measures taken to protect information and systems from adversaries. This is unfortunate, as IA should continue to include considerations such as proper system administration, system maintenance, and planning for power or equipment failures. IA should also encompass larger issues such as the degree to which systems actually meet user requirements for information delivery and access–in other words, does the system do what it needs to do to support the warfighter?

Current definitions of IA do not include the term computer network defense (CND) and the relationship between CND and IA is not clear. This may be changed in upcoming modifications to Joint and Army doctrine and policies. For many IA has come to be viewed as being *preventive* in nature while CND is considered to be *reactive*. Those measures taken in the absence of a specific threat (system administration procedures, backing up data) being considered IA, while the measures taken in response to identified deliberate attacks (implementing new firewall rules, disconnecting portions of networks, etc.) being considered CND. This dichotomy is reflected in the division of responsibility for IA and CND within DoD (this will be discussed later).

Perhaps more than any other area of IO, the areas involving the protection of information and information systems have generated numerous terms and concepts. In addition to IA, other terms are also widely in use in DoD. Information security (INFOSEC) includes aspects of computer and communications systems but also includes aspects not related to computers or electronic systems, for example, keeping printed classified material under proper control and protected by physical means. Communications security (COMSEC) involves the protection of information during transmission–primarily by the employment of cryptography. Computer security (COMPUSEC) entails security of computers and information stored on those computers. Critical infrastructure protection (CIP) includes protection of things like communications facilities, transmission media (fiber optic cable routes, microwave towers), and the commercial electric power grid.

OPERATIONS SECURITY

As mentioned earlier, OPSEC is considered primarily defensive in nature, but can include offensive aspects as well. Almost all activities associated with protecting friendly information, information systems, and communications from enemy exploitation could be considered examples of defensive OPSEC.

PHYSICAL SECURITY

Physical security is an important aspect of information operations as physical security is the first line of defense against access to our systems and information. Physical security is often an underrated aspect of defensive information operations within DoD as IO emphasis is directed to more technical concerns such as cryptography and network intrusion detection. All DoD classified networks are (or are at least supposed to be) protected by an outer layer of physical security in the form of facilities with controlled physical access (guards, keypads, combination locks). The stringency of this physical security increases in accordance with the classification level of the system involved. Any proposed interconnections between classified networks and other networks that may provide an inadvertent path allowing an adversary to bypass physical security measures should be thoroughly reviewed before implementation. This would include even a filtered connection between a classified and an Internet-connected network. Any situation in which an adversary could even attempt to access a critical network without first penetrating some form of physical security induces some level of risk. Strong physical security does not solve all problems though--physical security at the system perimeter does not provide protection from *insider attacks*.

ELECTRONIC WARFARE

The defensive aspects of EW include protection of electronic systems from attacks via electromagnetic pulse (EMP), prevention of enemy exploitation of friendly communications transmissions, and the prevention of enemy exploitation of information inadvertently transmitted via electromagnetic emanations. Electromagnetic emanations can radiate from things like copper network cables and computer monitors. Although requirements have been relaxed for certain situations in recent years, the intent of DoD TEMPEST standards is to decrease risk from electromagnetic emanations.[25]

COUNTERDECEPTION

The intent of counterdeception is to offset or even to take advantage of enemy efforts to deceive friendly forces. JP 3-13 states that counterdeception is primarily accomplished through maintaining accurate assessments of enemy posture and intent.[26] Curiously counterdeception does not include intelligence aspects of identifying enemy deception efforts.[27] Separating these two functions does provide a degree of security in preventing adversaries from determining that their deception efforts have been detected and determined to be acts of deception.

COUNTERPROPAGANDA

Like counterdeception, the intent of counterpropaganda is to offset or limit the effects of enemy propaganda efforts. Neither JP 1-02 nor JP 3-13 offers much information on counterpropaganda. An example of counterpropaganda would be the dissemination among friendly troops of information discrediting enemy propaganda efforts. An amusing example, would be the wide publication among deployed U.S. troops of information discrediting enemy radio broadcasts. For example, During Desert Storm Iraqi commentators could have asserted via radio broadcast that wives and girlfriends back home were being wooed by the likes of Tom Selleck and Bart Simpson. Informing U.S. troops of this particular broadcast would clearly discredit related Iraqi effort to demoralize U.S. troops. Many readers have undoubtedly read or heard this story and such a story was in fact included in reputable publications.[28] Even though it seems very believable, the story was none the less a hoax.[29] I include this example here because it says a lot about the power, and persistence, of misinformation and does provide ideas on how to actually counter enemy propaganda efforts.

COUNTERINTELLIGENCE

Counterintelligence (CI) consists of information and activities to protect against espionage, terrorism, and other activities of foreign intelligence organizations—in short countering adversary intelligence efforts. Counterintelligence includes four functions: operations; investigations; collection and reporting; and analysis, production, and dissemination.[30] IA and OPSEC can contribute to CI by protecting friendly information and information systems. Likewise CI can support other defensive IO areas by providing intelligence on adversary threats.

SPECIAL INFORMATION OPERATIONS

JP 3-13 includes SIO as an element of defensive IO; however, it would appear that most efforts warranting designation as SIO would be offensive in nature. An exception might be measures taken to counteract a network intrusion when it may be desirable to avoid tipping off the adversary that his actions have been detected. Considering these defensive measures as SIO should prevent information regarding these measures from being widely disseminated.

Information Operations Related Activities

Current Joint doctrine specifies two IO related activities: public affairs and civil affairs. *IO related* means that these activities are not directly considered IO, but have an impact on IO or could be supported by IO. The separation of these areas from other aspects of IO is to avoid suggestions that the U.S. would employ IO such as PSYOP in conjunction with public affairs or civil affairs.

PUBLIC AFFAIRS

Public affairs (PA) comprise DoD efforts to disseminate information via public or open channels. This includes information intended for consumption outside of DoD as well as information intended for specific audiences within DoD (also known as command information). Within DoD, use of PA for IO purposes is strictly limited to disseminating factual information to counter adversary deception or propaganda.[31] Using PA to disseminate false information violates U.S. laws, policy, and values. The mere allegation that DoD might use public media channels to spread misinformation, even if aimed at adversaries, was enough to force the disbanding of the short-lived Office of Strategic Influence (OSI). Press reports regarding OSI indicated this new organization would use foreign media channels for PSYOP and deception purposes. The result was that the Secretary of Defense quickly disbanded the organization.[32]

CIVIL AFFAIRS

Civil affairs (CA) activities promote effective relationships between friendly military forces and civilian authorities.[33] Such effective relationships would benefit from the exchange of information, especially information of a nature that would influence foreign civilian authorities to support, or to at least accept friendly military forces. Joint doctrine further defines CA as those activities that "involve application of civil affairs functional specialty skills"[34] (a rather circular definition). The qualification of CA as an IO related activity is somewhat dubious. At a minimum, employing PSYOP in support of CA carries the risk of discrediting those very CA efforts. CA relies on effective flows of information and other IO activities must be coordinated with CA activities to prevent one from unnecessarily detracting from the other. Beyond that, CA appears to be no more of an IO related activity than many other forms of military operations that are not considered to be IO.

ASSESSMENT OF CURRENT DOCTRINE

Current U.S. military IO doctrine lacks coherence and consistency. This not only causes confusion and obfuscation, but may also have a negative impact on IO organization and resource allocation. An assessment of current IO doctrine yields the following observations.

Diverse Mission Area Elements

All of the elements of a single mission area should bear a distinct relationship to one another. Elements of a single mission area should be similar in nature or yield similar results. As currently defined, IO is a very diverse mission area. So diverse in fact that some elements of IO are totally unrelated to one another. One example of this is PSYOP and IA--it is difficult to imagine any relationship between these two mission areas. Because a single field named "IO" exists, DoD attempts to create organizations and individual experts that can perform tasks across that entire field. With such a broad range of subject areas, it is difficult to develop IO expertise in the form of trained practitioners who are skilled in all areas of IO. The Army maintains a personnel management designation for IO officers known as Functional Area 30. The Army's intent is to develop officers who can coordinate all of the functions of IO. Since it would be very difficult to develop people with a high degree of skill in all areas, it is fortunate that the Army also maintains specialists in many of the component areas of IO. For example, the Army has officer specialties for information systems, PSYOP, public affairs, and civil affairs; as well as similar specialties for enlisted soldiers and warrant officers.

Overuse of the Term "IO"

IO is such a varied mission area that use of the generic term "IO" to describe specific IO component mission areas leads to confusion. The term IO is often used when it would be more descriptive to use the specific name of the component mission area. Frequently it appears that the term "IO" is used when it would be more appropriate to use the terms "PSYOP" or "deception." In other cases, the term "IO" is used when it would be more appropriate to use the term "electronic warfare" or the term "information assurance." Overuse of the term "IO" in lieu of the terms for specific component mission areas leads to a limited understanding of the diverse nature of IO missions.

IO as an Integrating Strategy

JP 3-13 describes an additional facet of IO–that of IO as an "integrating strategy."[35] When employed in this manner, IO is to ensure synchronization, coordination, deconfliction, and the maximum benefit from the various elements of IO. Theoretically IO would take the form of an integrating strategy at higher levels where multiple forms of IO would be coordinated. JP 3-13, nor any other document, describes the details of using IO as an integrating strategy or how the desired effects of the IO integration strategy are to be achieved. We do need an integrating strategy to ensure synchronization, coordination, deconfliction, and the maximum benefit from the various elements of IO. To in effect state that "IO is the integrating strategy for IO" leaves much to be desired. DoD has not fully developed the strategy, policies, concepts, and procedures to integrate the various aspects of IO and to integrate the various aspects of IO within broader operations.

Overemphasis on Computers

Another problem with Joint and Army IO doctrine is that it is influenced by a compelling tendency to focus on those aspects of IO involving computers. As discussed earlier, Joint and Army doctrine includes a diverse range of related areas (albeit some only slightly related). Despite the range of topics and issues, Joint and Army publications, military journals, and other documents tend to focus on computers vice, for example, deception. This tendency is likely a result of the pervasive presence of computers in our society. A large portion of our population uses computers on a daily basis and sees computer skills as a way to enhance employment and income. Not many in our military are in any way involved in military deception. Another factor is that developing computer based aspects of IO results in a large amount of business and research funded by DoD–military deception results in comparatively little DoD funding.

Merely Using Information is not Information Operations

As of the publication of FM 100-6 in 1996 the Army had a very broad interpretation of what constitutes IO. This interpretation was so broad that virtually any type of military operation could be considered an information operation. This early version of FM 100-6 includes "interacting with the global information environment"[36] as an aspect of IO. Today it is hard to conceive of any military endeavor that wouldn't involve interaction with the information environment. FM 100-6 includes a vignette describing how enterprising civil affairs officers developed a database that facilitated distribution of relief supplies to Kurdish refugees in 1991.[37] Although an excellent example of employing initiative and skill, of the Army benefiting from the civilian sector skills of Reserve component soldiers, and of using a computer-based information system this should not be considered an example of IO. U.S. Air Force doctrine also diverges from joint doctrine in that the Air Force uses a definition of IO that is much broader than the Joint definition. The U.S. Air Force has developed the term *information-in-warfare* to describe the collection and use of information to support peace and combat operations and the Air Force includes information-in-warfare as an element of IO.[38] Although I do not agree that *information-in-warfare* should be considered and aspect of IO, I do agree that we need terminology to describe using information within our operations vice employing *information warfare*. Merely using or effectively managing information, particularly information about our own forces and assets, should not qualify as IO.

Likewise gathering, processing, storing, disseminating and using generic intelligence should not qualify as IO. Gathering and using intelligence is as old as warfare itself. The U.S. in particular employs extensive computer systems, communications networks, electronics, and digital technology in intelligence activities, but using such resources in any activity does not necessarily make that activity part of IO. Admittedly, we will require extensive, sensitive, and detailed intelligence in order to conduct effective IO, but intelligence activities should not in and of themselves be considered IO.

Relationship between IA and CND

Some areas of Joint and Army IO doctrine are confusing and incoherent because of a poorly defined relationship between CND and IA. There are few, if any, CND concepts or activities that cannot be accounted for under the existing five component areas of IA yet CND essentially exists as a separate function. As mentioned earlier, some have come to view IA as being *preventive* and CND as being *reactive*. Considering IA as being only preventive in nature, IA would include things like virus protection, proper system administration procedures, firewalls, COMSEC, and other security measures. Then considering CND as being reactive, CND would include things like network intrusion detection, correlation of indicators, and directing countermeasures in response to identified intrusion attempts or other active situations. In reality preventive and reactive measures are so intertwined it is difficult to separate them. For example, a network administrator whose preventive measures have failed clearly should take reactive measures to counter specific intrusion attempts or other emerging security problems.

The view that CND and IA are identifiably separate areas of IO may have been a factor in assigning responsibility for these areas. IA is generally viewed as a Service, Agency, or program manager responsibility. Although no Service would deny responsibilities for CND, CND is specifically assigned as a mission to USSTRATCOM. This issue will be explored further under organization for IO. CND and IA bear a strong, if not inseparable relationship. Perhaps some in DoD are coming to an understanding of the relationship between IA and CND and perhaps even beginning to question if IA and CND are actually separate areas of responsibility. A grassroots phrase I have heard that generally meets with little disagreement is "you can't do CND without IA."

Over-hyping Computer Network Attack

Much has been written about DoD establishing computer network attack (CNA) as a mission area. Much of this writing ignores the extreme difficulties the U.S. would have in executing successful CNA (as currently defined as using primarily non-kinetic means). Because of this many false hopes for CNA have been created. Successful CNA will require detailed intelligence about specific enemy information systems. Details such as make, model, and version of hardware and software would be necessary. Gathering this information via means other than human intelligence may alert the enemy to any potential vulnerability. Physical access to the system or network, or some technologically advanced method to penetrate the system from afar, would be required. The attention we have devoted to CNA and other aspects of IO has no doubt alerted our potential adversaries of our intent to employ CNA if possible. For this reason, potential adversaries will likely place more focus on security of their systems or avoid becoming reliant on them altogether (of course not employing greater computerization may have a second order effect of making our adversaries less responsive and effective). Successful CNA is not impossible--only much more difficult than many may have been lead to believe.

The generation of false hopes for CNA is typified by the example of the Iraqi printer virus story that was widely disseminated in 1992. So the story goes, the U.S. was able to implant a virus in printers shipped to Iraq and intended to be part of an Iraqi military system. To many the idea of the U.S. implanting such a virus was believable and many of us no doubt wanted to believe it was true. Unfortunately the genesis for this story was a concocted story in a computer industry publication and intended to be a joke.[39] None the less, it was widely disseminated, embellished, attributed to DoD sources, picked up by major news outlets, and assumed to be factual.

Concept of Information Attack

As discussed earlier, one area in which Joint and Army doctrine is lacking is in the area of what the Air Force defines as *information attack*. Information attack is defined as "directly corrupting information without visibly changing the physical entity within which it resides."[40] Joint and Army doctrine tend to focus more on shutting down or damaging computers or network equipment vice exploiting some opening to inject misleading information. An example of information attack would be inserting false data into the data stream between an enemy sensor and enemy database of friendly unit locations. Executing an information attack would take detailed knowledge of a particular enemy system as well as specific knowledge of points at which false data could be injected. These challenges have likely resulted in the limited inclusion of the concept of information attack in Joint and Army doctrine. Despite these challenges the payoffs from information attack are potentially very significant.

Exploitation not included as a mission area

Exploiting an enemy information asset for intelligence purposes is not currently considered an aspect of IO in Joint and Army doctrine. If and when friendly forces gain awareness of an enemy information asset, and gather enough intelligence to take some action against that asset, friendly forces should carefully weigh options. Should they attack that enemy asset? Should the attack occur now or should they wait for more intelligence that might expand their options? Do they attack with kinetic means or do they attack the asset via electronic means such as jamming? Do they execute an information attack to eliminate the data or inject inaccurate data into the system? Do they allow the enemy system to continue to operate and then attempt to exploit that asset for intelligence purposes? The need to balance exploiting enemy information systems vice attacking and destroying or degrading that enemy system (by whatever means), or taking some action that would indicate to an enemy that a particular vulnerability exists in an enemy system, is why exploitation should be considered part of IO. The valuable intelligence gained by the allies after they were able to break the German Enigma cryptographic system is an excellent example of exploiting information systems for intelligence purposes vice attacking those same systems in order to destroy or degrade them.

CURRENT ORGANIZATION FOR IO

Responsibilities for IO are currently divided between the Office of the Secretary of Defense, the Services, Defense agencies, the regional Unified Combatant Commanders (UCCs), USSTRATCOM, and USSOCOM. There is no single hierarchical "chain of command" responsible for all aspects of IO. Although no such hierarchy of responsibility is proposed, other changes should be considered. Minor adjustments to responsibilities for IO would improve U.S. ability to execute the various missions that comprise IO. Through an assessment of organizational responsibilities for the various aspects of IO, the U.S. military could achieve a more effective allocation of missions. This assessment could lead to clearer lines of responsibility, elimination of unnecessary redundancy, and increased cooperation in achieving IO objectives.

USSTRATCOM IO Functions

On 1 October 2002 major portions of USSPACECOM were subsumed by USSTRATCOM and USSPACECOM was eliminated as a separate UCC. USSTRATCOM inherited responsibility for IO missions that were formerly the responsibility of USSPACECOM. When still assigned to USSPACECOM these missions may not have been clear as the Center for Strategic and International Studies assessed USSPACECOM information security and infrastructure protection missions as "general" and "nebulous."[41] Along with commensurate unified command plan (UCP) responsibilities, USSTRATCOM now has two subordinate commands charged with specific IO responsibilities—the Joint Task Force Computer Network Operations (JTF-CNO) and the Joint Information Operations Center (JIOC). USSTRATCOM also inherited another responsibility from USSPACECOM–that of coordinating IO in support of *Operation Enduring Freedom*. Since that time, USSTRATCOM has been assigned broader responsibilities for IO within DoD.

JOINT TASK FORCE-COMPUTER NETWORK OPERATIONS

The Joint Task Force Computer Network Operations (JTF-CNO) is charged with computer network defense (CND) and computer network attack (CNA). USSTRATCOM defines the CNA mission as "to coordinate, support and conduct . . . computer network attack operations in support of regional and national objectives."[42] USSTRATCOM defines the CND mission as "to defend DOD computer networks and systems from any unauthorized event."[43] To perform the CND mission, USSTRATCOM is assigned components from the Services and the Defense Information Systems Agency (DISA): the Army's Computer Emergency Response Team (ACERT–part of the Army's 1st Information Operations Command), the Marine Forces-Integrated Network Operations (MARGOR-INO), the Navy Component Task Force-Computer Network Defense (NCTF-CND), the Air Force Forces-Computer Network Operations organization (AFFOR-CNO), and DISA's DOD Computer Emergency Response Team (DOD CERT).[44] A factor that limits the effectiveness of this particular organization is that JTF-CNO and the components that are assigned are not responsible for the operation of the networks and systems for which they are responsible to defend. For example, within the Army responsibility for operating networks and lies with the Army's new Network Command (NETCOM); however, the ACERT–the Army component under OPCON of the JTF-CNO–is not a part of NETCOM. In this example, the responsibility for operating Army networks is not consolidated with the responsibility for protecting those networks from adversaries. The DoD-level organization with responsibility for operating networks and systems across unified command and Service boundaries is DISA, yet JTF-CNO is a USSTRATCOM element. DoD attempts to overcome some of the friction that may arise between JTF-CNO and DISA by dual-hatting the Deputy Director of DISA as the Commander, JTF-CNO. The DoD Computer Emergency Response Team (DoD CERT), a DISA element, is also under tactical control of JTF-CNO. JTF-CNO is also collocated with the DoD CERT and DISA's Global Network Operations and Security Center (GNOSC). If not for this collocation and dual-hatting of a senior officer it is easy to imagine circumstances under which organizational conflict between the JTF-CNO and DISA could develop. The Army has taken similar measures and has collocated elements of the 1st IO Command and NETCOM.

JOINT INFORMATION OPERATIONS CENTER

The Joint Information Operations Center (JIOC), formerly under USSPACECOM, is also now a subordinate element of USSTRATCOM. The JIOC "is responsible for the integration of Information Operations (IO) into military plans and operations across the spectrum of conflict."[45] The JIOC's mission is to "assist in planning, coordinating and executing information operations."[46] The JIOC does not have any forces or elements assigned that can actually execute IO missions and the JIOC itself has only IO plans officers and technical experts within various IO fields assigned as part of its organization. Several issues become apparent with the JIOC's assigned functions and its location within the organizational hierarchy. USSTRATCOM possesses one organization responsible for executing major IO missions (the JTF-CNO responsible for CND and CNA) and a different organization–the JIOC–responsible for full spectrum IO planning and coordination. United States Strategic Command performs high-level IO planning and coordinating functions, yet major IO organizations are not a part of USSTRATCOM. For example, the Army's only active duty PSYOP unit is assigned to a different UCC—the Army's 4th PSYOP Operations Group (4th POG) is assigned to USSOCOM.

SPACE AND INFORMATION OPERATIONS ELEMENT

In an effort to provide better support to USCENTCOM as the supported UCC for Operation Enduring Freedom, USSPACECOM established a Space and Information Operations Element (SIOE) and located elements of the SIOE at HQ USCENTCOM.[47] The SIOE became an element of USSTRATCOM on 1 October 2002 as part of the realignment of unified commands. This is an interesting arrangement if one considers all of the aspects of IO as currently defined. All of the forces that would execute IO missions are not assigned to USSTRATCOM. It would seem more logical that USCENTCOM would establish an SIOE and that the SIOE would clearly be part of the USCENTCOM staff. USSTRATCOM would then support the SIOE by providing staff augmentation to USCENTCOM to assist in planning and coordinating CND, CNA, and space support (communications, surveillance, missile warning). Similarly, USSOCOM would provide PSYOP and CA planners or liaison officers. Under this arrangement USCENTCOM would be remain clearly overall responsible for planning, coordinating, and executing IO in support of Operation Enduring Freedom.

USSOCOM IO functions

The major PSYOP units within DoD are assigned to or under the tactical control of USSOCOM. This includes the Army's 4th POG, as previously mentioned, and the 193d Special Operations Wing (SOW) of the Pennsylvania Air Nation Guard. The 193 SOW operates all Commando Solo aircraft within the DoD. Commando Solo aircraft are equipped with advanced electronics that allow them to jam media broadcasts (television, radio) and to transmit similar broadcasts conveying information in support of U.S. efforts. Although USSOCOM is assigned these significant forces, USSOCOM does not have broad IO responsibilities across DoD or for coordinating IO outside of USSOCOM operations.

Regional Unified Combatant Commander Responsibilities

Generally, regional UCCs are responsible for conducting IO within their geographic areas of responsibility. Typically regional UCCs establish IO cells on their staffs in accordance with concepts outlined in JP 3-13. These IO cells are normally under the UCC J3 and are formed with representation from appropriate elements from across the UCC staff and subordinate units. Regional UCC staffs can also be augmented with expertise from other UCCs or from the Services. Specific IO forces can be assigned or allocated to a particular UCC. Under current policy, regional UCC's are not granted authority to execute CNA–the President and Secretary of Defense retain this authority. This is a minor limitation, and current doctrine is sufficient to enable the use of CNA within a regional UCC geographic area of responsibility.

DISA responsibilities

DISA is responsible for "planning, developing, fielding, operating, and supporting command, control, communications, and information systems."[48] The DoD Computer Emergency Response Team (DoD CERT) is an element of DISA and serves as the primary focal point for identifying vulnerabilities and viruses affecting DoD networks. The CERT is responsible for then disseminating information regarding preventive measures that should be taken to prevent problems related to these viruses and vulnerabilities. DISA also has a major element–the Global Network Operations and Security Center (GNOSC)–specifically responsible for monitoring and operating networks and other communications under DISA's purview. DISA considers IA one of its "core mission areas"[49] and DISA performs many functions in support of IA throughout DoD. In spite of this extensive involvement with IA across DoD, DISA is not assigned and does not claim overall responsibility within DoD for planning, implementing, or otherwise executing IA. An overlap between the CND mission of USSTRATCOM and the IA mission of DISA is also apparent.

NSA responsibilities

NSA performs IO missions in two major areas: IA and signals intelligence (SIGINT). Regarding the IA mission, NSA "provides the solutions, products and services, and conducts defensive information operations, to achieve information assurance for information infrastructures critical to U.S. national security interests."[50] As part of this mission, NSA manages cryptographic systems for DoD. NSA also provides other support in the form of technical experts and "Red Teams" to assist DoD elements in protecting computer networks and other communications. NSA's other major mission area–that of SIGINT–involves intercepting and decoding foreign communications. As noted earlier, under current DoD IO definitions any functions such as intercepting and decoding communications would not be considered as IO functions. To foster cooperation between NSA and other DoD organizations, and to ensure effective NSA support to those other organizations, NSA maintains permanent liaisons stationed with the UCCs and at other DoD agencies.

Defense-wide Information Assurance Program

The Defense-wide Information Assurance Program (DIAP) exists as a staff function under the Deputy Assist Secretary for Space and Information Operations (DASD (S&IO)) within the office of the Assistance Secretary of Defense for Command, Control, Communications, and Intelligence (ASDC3I). The DIAP's stated mission is "is to ensure the Department of Defense's vital information resources are secured and protected by unifying/integrating IA activities to achieve information superiority."[51] Since the DIAP exists at the Office of the Secretary of Defense level, the DIAP is the highest level organization to which responsibility for IA within DoD can be fixed. Despite the emphasis placed on the DIAP when it was formed in 1998, the Government Accounting Office cited failures of the DIAP in a 2001 report.[52] These failures were at least partially attributed to "management challenges" including staffing, guidance, and oversight.[53] Some of these shortcomings may stem from the fact that the ASDC3I has relatively little control over resources. Prior to leaving office the previous ASDC3I, Mr. Arthur Money, proposed elevating his position to under secretary level and transferring some fiscal control to that position.[54] Although the intent of this move was to better ensure interoperability, strengthening the C3I position would also enhance the ability of the DIAP to manage IA across DoD.

Service Responsibilities

Each Service is responsible for establishing IO capabilities that can then be used under the auspices of one of the UCCs in support of strategic or operational objectives. Each Service has responsibility for ensuring systems and capabilities developed under its purview include measures to counter enemy attempts to degrade or damage those systems through the use of IO. Each Service is also responsible for fielding its own offensive IO capabilities for example in the form of EW systems. Each of the Services has some form of PSYOP capability ranging from the production of PSYOP materials to the means to disseminate those materials.

Each Service is currently in the process of a reorganization of its network and communications organization and several Services have major network reconfiguration or consolidation efforts underway. A common facet of each of the Service efforts is a centralization of network monitoring for both availability and security purposes. The Army has formed a new organization—Network Command or NETCOM—that reports directly to the Army's G6. The Air Force is consolidating network responsibilities for networks operating at the classification level of SECRET and below at the Major Command (MAJCOM) level. The USAF consolidation initiative will also centralize certain network services (e.g. email) at the MAJCOM level. The most major among Service network consolidation and reorganization efforts is the Department of the Navy's Navy-Marine Corps Intranet (NMCI). Under NMCI the Navy and Marine Corps will not only centralize network functions including security monitoring, but also outsource the operation of fixed networks. Across the Services what is occurring is a consolidation of network operation and security functions that is not necessarily conducive to exercising control at levels higher than the Service level (i.e. across the Services at the DoD level). Rather than a single coherent network under control of a DoD-level organization, what is developing is a set of cooperative Service networks.

ASSESSMENT OF CURRENT ORGANIZATION

IO organization within DoD is currently suboptimal and marked by a lack of consolidation of responsibility for closely related functions. At the same time, there are examples of the centralization of responsibility for certain IO missions with responsibilities for other areas of IO that are not closely related. There area also examples where responsibility for certain missions has been assigned yet the allocation of forces does not reflect the assignment of responsibilities. An assessment of DoD's organization relating to IO yields the following observations.

Responsibility for operation and protection not consolidated

As noted earlier, responsibility for operating networks and systems is split between DISA, the Services, and the regional unified commands. Responsibility for security of those same networks and systems is split between DISA, the Services, the regional unified commands, and USSTRATCOM. DoD has higher level responsibilities in both realms, with additional special emphasis on security through the DIAP. In particular the split of responsibility between DISA and USSTRATCOM is most poignant—DISA has responsibility for providing network services and maintains IA as one of its core programs, yet USSTRATCOM is responsible for "computer network defense." The same situation basically exists within the Army with responsibility split between the 1st IO Command and NETCOM.

Responsibility for nonkinetic and kinetic attack not consolidated

If offensive IO is to yield the benefits many have touted, IO methods must be considered as options along with kinetic forms of attack. Regional UCC's have clear and direct control over kinetic forms of attack within their AORs, but this is not the case with offensive IO. Existing PSYOP units are assigned to USSOCOM (but of course could be task organized under any particular UCC control). Any existing CNA capability would be assigned to USSTRATCOM or under some form of USSTRATCOM control. The JIOC, now a USSTRATCOM element, deploys teams to support regional UCCs and has responsibility for "[assisting] in planning, coordinating and executing information operations."[55] Currently any execution of IO would require extensive coordination between multiple organizations and multiple UCCs.

Deconflicting attacks and exploitation

The requirement to deconflict CNA and EW with exploitation efforts is paramount. If this deconfliction doesn't occur, efforts to destroy, degrade, or temporarily disable adversary communications or information systems could impede exploitation efforts that are actually yielding intelligence more valuable than any gain from destroying or otherwise affecting that same target. In the future when our capabilities are more fully developed, efforts to attack enemy systems could also interfere with our ability to inject false information into those same systems in support of deception efforts. Ostensibly, these various efforts would be coordinated in the UCC IO Cell; however, the establishment of elements under other unified command control (like an SIOE) creates other entities that must be included in coordination rather than simplifying this process.

Responsibility for PSYOP and other IO areas unnecessarily consolidated

While responsibility for closely related areas of IO are not consolidated within DoD, for example IA and managing networks, there is a tendency to consolidate responsibility for areas that are not closely related. An example is assigning responsibility for IO as a monolithic mission to USSTRATCOM. USSTRATCOM inherited the CND and CNA missions, and the JIOC from USSPACECOM on 1 Oct 2002. As part of that realignment, DoD announced that USSTRATCOM would assume responsibility for broad-based IO on a global basis. This probably stemmed from a desire to place responsibility for all of the elements of IO as currently defined under a single unified commander. CND, CNA, and PSYOP are significantly different functions. So different, there is little need to consolidate responsibility under a single functional UCC. Responsibility for executing CND, CNA, or PSYOP in a particular geographic area should remain the responsibility for the respective *regional* UCC. Consolidating responsibility for these various areas under a single *functional* UCC yields little benefit.

Coordinating and deconflicting Red Teaming

Red Teaming is valuable method to determine vulnerabilities and weaknesses in friendly networks and systems. The current fractured state of responsibility for operations and security of networks and systems within DoD does not support effective employment of Red Teaming. When Red Teams are employed, managers must decide who will be notified in advance. In the past there has been a tendency to use Red Teams as method to test the response of targeted organizations rather than to simply identify and correct vulnerabilities. What has sometimes been reported in the past is that targeted organizations don't detect, respond to, or report the activities of Red Teams.[56] There is often however another result. Organizations can detect the activities of the Red Team and then spend valuable time reacting to the Red Team's activities. A sort of "boy of cried wolf syndrome" can result—if organizations detect unusual activity after several experiences with unannounced Red Team activity they pass off the current activity as that of a Red Team. When Red Teams are employed, DoD should follow a policy of notifying all organizations, network manager, system administrators, network security managers involved. Red Teaming should be used extensively to detect vulnerabilities and weaknesses in networks and systems, but it should be used primarily to identify and correct vulnerabilities and secondly to train those operating systems and networks. It should only be used to test response on a very limited basis.

REVISIONS TO ARMY FIELD MANUAL 100-6 (FM 3-13 DRAFT)

At the time of writing the Army is on the verge of replacing FM 100-6 with FM 3-13 (also entitled *Information Operations*). FM 3-13 is currently in final draft form. FM 3-13 (DRAFT) is a significant improvement over FM 100-6, but until formally issued all of the proposed changes cannot be assumed to be official. FM 3-13 (DRAFT) reflects a more mature and sophisticated understanding of IO within the Army. FM 3-13 reflects consistency with the Joint Doctrine publication numbering system (i.e. JP 3-13) and for the most part copies Joint terminology exactly–but there are differences. In several places FM 3-13 admittedly differs from Joint doctrine and so states.[57] An examination of FM 3-13 (DRAFT) reveals many positive changes, but the document still contains some items that carry over some of the former confusion and lack of clarity of previous documents.

Among the positive changes in FM 3-13 (DRAFT) are the definition of information superiority as a relative operational advantage over an adversary–something still lacking in Joint doctrine.[58] FM 3-13 (DRAFT) also defines IO as being executed "across the spectrum of conflict"[59] thereby avoiding the "IW is wartime IO" complications. This new draft also includes exploitation as an aspect of IO and clearly includes CNE as an element of CNO.[60] Gone is the consideration of merely using information as being considered an example of IO. FM 3-13 thoroughly covers the integration of IO with other forms of operations and includes a great deal of guidance on how to accomplish this integration at the tactical and operational levels.

Among the limitations with FM 3-13 (DRAFT) is continued lack of clarity on the relationship between IA and CND. FM 3-13 (DRAFT) identifies CND as being a "core" IO function, but limits IA to a "supporting" role.[61] FM 3-13 (DRAFT) defines CND as being "enabled by IA,"[62] but then contradictorily states that "IA incorporates CND"[63] and that "IA uses a defense in depth that includes CND."[64] Unless changed prior to final publication, the new FM 3-13 will not be clear as to whether IA includes CND, CND includes IA, or whether some other relationship exists. The new FM 3-13 does include the concept of *information attack*, but includes information attack under exploitation rather than combining information attack with other forms of attack (CNA, EW, physical attack).

FM 3-13 (DRAFT) continues some of the overemphasis on computers and overhyping of CNA capabilities found in older documents. In identifying threats in the information environment, FM 3-13 (DRAFT) limits threats to those that are computer-based and fails to include other forms of threats to our information, information systems, and associated ability to execute successful operations.[65] The document also contains a poor example of what is possible within the realm of CNA (issuing a command to short out a power supply).[66] Despite these shortcomings and those mentioned in the previous paragraph, FM 3-13 (DRAFT) is an admirable effort on the part of the Army and a significant improvement over FM 100-6. If enacted as currently written FM 3-13 will in fact implement some of the recommendations that follow.

RECOMMENDATIONS

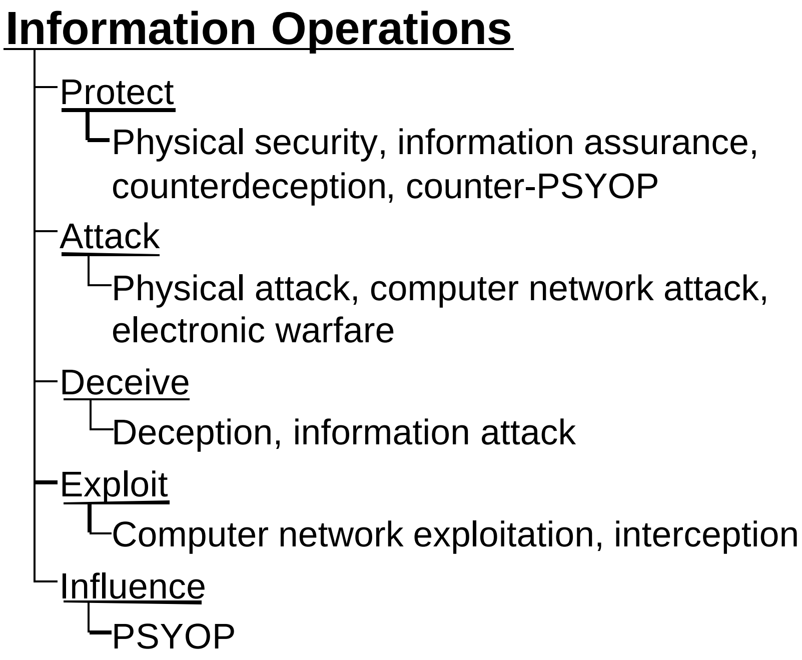
United States IO effectiveness would benefit from changes to terminology, doctrine, and philosophy. First, DoD should implement a new taxonomy for IO and its component mission areas. DoD should abolish the offensive, defensive, IO-related categorizations described earlier. DoD should subdivide the IO function into five functional areas: *protect, attack, deceive, exploit, and influence*. The *protect* function would include activities to protect information including measures that protect our own information and information systems. The *attack* function would include offensive measures to destroy, degrade, or deny enemy information or information systems. The attack function would include kinetic measures; electronic measures such as jamming and EMP; as well as CNA. The *deceive* function would include tactical/strategic deception and *information attack* as described earlier. *Exploitation* would encompass efforts to intercept, decrypt, monitor, or otherwise access enemy information. *Influence* would include those functions currently considered as PSYOP and truth projection, but would only include those types of efforts when aimed at enemy populations.

Specifically excluded from the influence function would be PA and CA. The risks of damaging U.S. influence, prestige, and credibility by indicating the perception of the use PSYOP or deceptive information on our own or friendly populations is too great. Such actions are so contrary to U.S. values, so opposed by our own population, and so potentially damaging to U.S. efforts that any suggestion of the possibility of a linkage between PA and CA to PYSOP should be eliminated. For this reason, PA and CA should not be considered IO-related activities at all. That said, PA and CA must be coordinated with IO and planners must consider the effects of these different areas upon one another.

Joint and Army doctrine should include the concept of information attack as already developed by the USAF. Although physically and technically very difficult, the function of injecting false information into enemy communications transmissions, databases, or other information stores should be included within IO. The payoffs from successful information attacks are potentially large and presumably carry relatively little risk for friendly forces.

Joint and Army doctrine should eliminate CND as a mission area and include current CND concepts under a strengthened concept of IA. The confidentiality, integrity, and availability components of IA comprise the essential elements of network and system security and therefore those of CND. The interpretation of that the availability component of IA includes things like proper system administration, backups, system maintenance should be emphasized. In the heat of battle, whether a system is unavailable because of an enemy attack or because it failed because of poor system administration may be of little consequence. Organizations with "CND" in their names could continue to exist, but interpretations of CND as something separate from IA should be discontinued.

Implementing these recommendations would result in a new taxonomy for IO. This taxonomy would include five main component areas as described earlier. The five main component areas would contain the functions indicated in the figure below.


Information Operations
Protect
Physical security, information assurance, counterdeception, counter-PSYOP
Attack
Physical attack, computer network attack, electronic warfare
Deceive
Deception, information attack
Exploit
Computer network exploitation, interception
Influence
PSYOP

RECOMMENDED TAXONOMY FOR INFORMATION OPERATIONS MISSIONS

DoD should implement several organizational changes to improve the effectiveness of IO as a means to accomplish U.S. national security objectives. First, steps should be taken to more tightly integrate targeting for CNA, EW, physical attack by kinetic means, and exploitation. CNA and EW targeting must be closely coordinated with kinetic targeting in order to ensure the best solution is employed against a particular target. DoD must also implement processes to deconflict exploitation with other forms of targeting in order to prevent the destruction or degradation of targets that could have been exploited to greater benefit. Simplifying our organization for IO would promote the necessary integration and create an environment more conducive to deconflicting the various missions within IO.

DoD should consolidate at a high level the responsibilities for the operation of networks and information systems with the responsibilities for protecting those assets. This would not only combine responsibility for operating networks with network security, but also create an environment that would simplify network monitoring, incident reporting, and the use of Red Teaming. DoD should consider assigning these responsibilities to a unified commander up to and including moving DISA under that unified commander. This would essentially entail designating a unified commander for information. This would not necessarily entail assigning

PSYOP, CNA, and EW to that UCC, but responsibility for operation and protection of our own information systems should be primary candidates for consolidation under a functional UCC. DoD should weigh this option against an option strengthening DISA's role for IA within DoD. The Army should take similar measures to consolidate responsibilities currently split between the 1st IO Command and NETCOM.

Throughout its various organizations DoD should implement a policy of consolidating responsibility for the operation and security of individual information systems or communications assets at all levels. Currently there are many instances within DoD where these responsibilities are split between different entities within the same organization. Those responsible for operating systems should also be responsible for the security of those systems. At the lowest levels, this policy would result in situations where system administrators are directly responsible for systems security. Situations where system administrators are not held accountable for security must be eliminated.

DoD should examine UCC roles associated with planning, coordinating and executing IO–particularly the roles of USSTRATCOM and USSOCOM. If a UCC is assigned a full spectrum IO responsibility or responsibility for particular areas of IO, then associated units should be transferred to that UCC. Although many factors undoubtedly affected past organizational decisions, DoD emphasis on transformation creates an environment where IO organizations and responsibilities could be realigned based on a long-term view and with an emphasis on effectiveness. In association with any reassignment of missions, DoD must realign resources in the form of personnel, units, and budgets. In particular, DoD should consolidate responsibility for PSYOP by combining responsibility for planning and integrating PSYOP with responsibility for actually executing PSYOP missions.

CONCLUSION

Information Operations will continue to be an important part of U.S. national military strategy. At present the U.S. possesses unprecedented military power relative to potential adversaries. The advanced state of U.S. integration of technology into military capabilities is a major factor in having achieved that advantage. The U.S. will increase the use of technology in the form of smart weapons systems, sensor-to-shooter integration, and advanced communications. Our adversaries will likely also increase their use of technology for military purposes. The role of information as an element of national power will also increase. DoD must come to a more advanced and sophisticated understanding of the elements of IO and more effectively execute IO missions in pursuit of national goals. DoD should examine our organization for IO and make changes that consolidate responsibilities for similar missions, establish simplified arrangements for coordinating different IO missions, facilitate the integration of IO into the full range of military operations in pursuit of national goals, and gain the maximum benefit from our IO capabilities.

IO is not necessarily a new aspect of warfare and one can argue that IO has always been a part of warfare. For example, on the first day of World War I a British cable ship severed German undersea telegraph cables dredged up from the North Sea floor near the German and Dutch borders.[67] The British had originally planned to execute this measure in 1912. The British had *detailed intelligence* and this action was *part of a larger strategic plan*. The British made a decision to *attack* and *destroy* the cable by severing it. The British employed a specialized capability--one of their own cable-laying ships--to sever the cable. Perhaps *exploitation* of the communications transmitted over the cable was not physically possible or perhaps that option was considered and discarded. One effect of the destruction of this cable was that Germany then had to rely on radio transmissions for any instantaneous communications--radio transmissions that the British could now intercept and exploit. Computers, computer networks, digital communications, advanced electronics change some of the means and methods, but the basic principles of IO remain unchanged. The U.S. should implement basic fundamentals to define and categorize IO, lay out clear IO doctrine, and simplify IO organization in order to gain maximum return from this aspect of warfare–an aspect in which the U.S. has the potential to retain significant advantages for the foreseeable future.

WORD COUNT = 11151

ENDNOTES

[1] Henry H. Shelton, Joint Vision 2020 (Washington: Joint Staff, June 2000), 2-3.

[2] Ibid., 28.

[3] U.S. Joint Chiefs of Staff, Joint Doctrine for Information Operations, Joint Publication 3-13 (Washington: Joint Staff, 9 October 1998), I-9.

[4] U.S. Joint Chiefs of Staff, Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02 (Washington: Joint Staff,12 April 2001), 211.

[5] Shelton, Joint Vision 2020, 8.

[6] U.S. Joint Chiefs of Staff, Joint Doctrine for Information Operations, I-1.

[7] Ibid., I-9 – I-10.

[8] Ibid., GL-9.

[9] U.S. Joint Chiefs of Staff, Department of Defense Dictionary of Military and Associated Terms, 153.

[10] Mark Thompson., "America's Ultra-secret Weapon," Time,19 January 2003; available from <http://www.time.com/time/covers/1101030127/nmicro.html>; Internet.; accessed 2 February 2003.

[11] U.S. Joint Chiefs of Staff, Department of Defense Dictionary of Military and Associated Terms, 352.

[12] Ibid., 332.

[13] Randal A. Dragon, Wielding the Cyber Sword: Exploiting the Power of Information Operations, Strategy Research Project (Carlisle Barracks: U.S. Army War College, 13 March 2001), 16.

[14] Bruce Schneier, Secrets and Lies: Digital Security in a Network World (New York: John Wiley and Sons, 2000), 39.

[15] U.S. Joint Chiefs of Staff, Department of Defense Dictionary of Military and Associated Terms, 91.

[16] Ibid., 91.

[17] U.S. Joint Chiefs of Staff, Joint Doctrine for Electronic Warfare, Joint Publication 3-51. (Washington: Joint Staff, 7 April 2000), IV-4.

[18] Ibid., IV-4.

[19] United States Strategic Command, "Joint Task Force-Computer Network Defense"; available from <http://www.stratcom.af.mil/factsheetshtml/jtf-cno.htm>; Internet; accessed 2 Feb 2003.

[20] U.S. Joint Chiefs of Staff, Department of Defense Dictionary of Military and Associated Terms, 404.

[21] Ibid., 118.

[22] Ibid., 321-322.

[23] Ibid., 210.

[24] U.S. Joint Chiefs of Staff, Joint Doctrine for Information Operations, I-9.

[25] Deborah Russell and G.T. Gangemi Sr., Computer Security Basics (O'Reilly and Associates: Sebastopol, CA, 1991) 253-255.

[26] U.S. Joint Chiefs of Staff, Joint Doctrine for Information Operations, III-5 to III-6.

[27] U.S. Joint Chiefs of Staff, Department of Defense Dictionary of Military and Associated Terms, 104.

[28] Dorothy E. Denning, Information Warfare and Security (Reading, MA: Addison-Wesley, 1999), 7.

[29] Snopes.com., "Baghdad Betty," Urban Legends Reference Pages; available from <http://www.snopes.com/radiotv/radio/baghdad.htm>; Internet; accessed 25 January 2003.

[30] U.S. Joint Chiefs of Staff, Department of Defense Dictionary of Military and Associated Terms, 105.

[31] U.S. Joint Chiefs of Staff, Joint Doctrine for Information Operations, III-7.

[32] Gerry J. Gilmore,"Strategic Influence Office 'Closed Down,' Says Rumsfeld" Armed Forces Information Service, 26 February 2002; available from <http://www.defenselink.mil/news/Feb2002/n02262002_200202263.html>; Internet; accessed 2 February 2003.

[33] U.S. Joint Chiefs of Staff, Department of Defense Dictionary of Military and Associated Terms, 70.

[34] Ibid., 70.

[35] U.S. Joint Chiefs of Staff, Joint Doctrine for Information Operations, I-3.

[36] Department of the Army, Information Operations, Field Manual 100-6 (Washington, D.C.:U.S. Department of the Army, August 1996), GL-7.

[37] Ibid., 3-13.

[38] Department of the Air Force, Information Operations. Air Force Doctrine Directive 2-5 (Washington, D.C.: Department of the Air Force, 4 January 2002), 31.

[39] Denning, 5-6.

[40] Sheila E. Widnall and Ronald R. Fogleman, "Cornerstones of Information Warfare," 1995; available from <http://www.af.mil/lib/corner.html>; Internet; accessed 16 December 2002.

[41] Arnaud de Borchgrave, Frank J. Cilluffo, Sharon L. Cardash, and Michele M. Ledgerwood, Cyber Threats and Information Security: Meeting the 21st Century Challenge (Washington, D.C.: Center for Strategic and International Studies, May 2001), 15.

[42] USSTRATCOM Web Site 2 Jan 2003 http://www.stratcom.af.mil/factsheetshtml/ jtf-cno.htm.

[43] Ibid.

[44] Ibid.

[45] United States Strategic Command, "Information Operations;" available from <http://www.stratcom.af.mil/factsheetshtml/Information%20Operations.htm >; Internet. accessed 2 Feb 2003.

[46] Ibid.

[47] Ralph E. Eberhart, Statement of GEN Ralph E. Eberhart to the House Armed Services Committee, statement presented to the House Armed Services Committee,14 March 2002; available from <http://www.defenselink.mil/dodgc/lrs/docs/test02-03-14Eberhart.rtf>; Internet; accessed 3 January 2003.

[48] Defense Information Systems Agency, "DISA Mission and Vision," 10 June 2002; available from <http://www.disa.mil/main/missman.html>; Internet; accessed on 3 January 2003.

[49] Ibid.

[50] U.S. President, Executive Order, "Executive Order 12333–United States Intelligence Activities," Federal Register 46 (4 December 1981): 200.

[51] Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, "Defense-Wide Information Assurance Program;" available from <http://www.c3i.osd.mil/ org/sio/ia/diap/>; Internet; accessed 4 Jan 2003.

[52] GAO "Progress and Challenges to an Effective Defense-wide Information Assurance Program" March 2001, page 12. Available at http://www.gao.gov/new.items/d01307.pdf. Accessed 26 Jan 2003.

[53] General Accounting Office, Progress and Challenges to an Effective Defense-wide Information Assurance Program (Washington, D.C.: U.S. General Accounting Office, March 2001), 20; available from <http://www.gao.gov/new.items/d01307.pdf>; Internet; Accessed 26 January 2003.

[54] George I. Seffers, "Defense CIO Seeks a Promotion" Federal Computer Week, 11 December 2000; available from <http://www.fcw.com/fcw/articles/2000/1211/news-cio-12-11-00.asp>; Internet; accessed 16 February 2002.FCW, 11 Dec.

[55] United States Strategic Command, "Information Operations."

[56] General Accounting Office, 19.

[57] Department of the Army, Information Operations, Field Manual 3-13 (FINAL DRAFT) (Washington, D.C.:U.S. Department of the Army, August 1996), 1-10, 1-13.

[58] Ibid., 1-10.

[59] Ibid., 1-19.

[60] Ibid., 1-14 to 1-17.

[61] Ibid., 1-14.

[62] Ibid., 2-10.

[63] Ibid., 2-12.

[64] Ibid., 2-13.

[65] Ibid., 1-14.

[66] Ibid., 2-8.

[67] David Kahn, The Codebreakers (New York: Scribner, 1967, 1996) 266-267.

BIBLIOGRAPHY

Assistant Secretary of Defense for Command, Control, Communications, and Intelligence. "Defense-Wide Information Assurance Program." Available from <http://www.c3i.osd.mil/org/sio/ia/diap/>. Internet. Accessed 4 Jan 2003.

Bateman, Robert L., ed. Digital War: A View from the Front Lines. Novato, CA: Presidio Press, 1999.

Best, Carole N. Computer Network Defense and Attack: Information Warfare in the Department of Defense. Strategy Research Project. Carlisle Barracks: U.S. Army War College, 10 April 2001.

Burnett, Peter L., Jr. Information Operations. Strategy Research Project. Carlisle Barracks: U.S. Army War College, 9 April 2002.

Campen, Alan D. and Douglas H. Dearth, eds. Cyberwar 2.0: Myths, Mysteries and Reality. Fairfax, VA: AFCEA International Press, 1998.

Cheeseman, Curtis P. Information Operation–Harnessing the Power. Strategy Research Project. Carlisle Barracks: U.S. Army War College, 8 April 2002.

de Borchgrave, Arnaud, Frank J. Cilluffo, Sharon L. Cardash, and Michele M. Ledgerwood. Cyber Threats and Information Security: Meeting the 21st Century Challenge. Washington, D.C.: Center for Strategic and International Studies, May 2001.

Defense Information Systems Agency. "DISA Mission and Vision." 10 June 2002. Available from <http://www.disa.mil/main/missman.html>. Internet. Accessed on 3 January 2003.

Denning, Dorothy E. Information Warfare and Security. Reading, MA: Addison-Wesley, 1999.

Department of the Air Force. Information Operations. Air Force Doctrine Directive 2-5. Washington, D.C.: U.S. Department of the Air Force, 4 January 2002.

Department of the Army. Information Operations. Field Manual 100-6. Washington, D.C.: U.S. Department of the Army, August 1996.

Dragon, Randal A. Wielding the Cyber Sword: Exploiting the Power of Information Operations. Strategy Research Project. Carlisle Barracks: U.S. Army War College, 13 March 2001.

Eberhart, Ralph E. Statement of GEN Ralph E. Eberhart to the House Armed Services Committee. Statement presented to the House Armed Services Committee. 14 March 2002. Available from <http://www.defenselink.mil/dodgc/lrs/docs/test02-03-14Eberhart.rtf>. Internet. Accessed 3 January 2003.

General Accounting Office. Information Security: Computer Attacks at Department of Defense Pose Increasing Risks. Washington, D.C.: U.S. General Accounting Office, May 1996. Available from < http://www.gao.gov/archive/1996/ai96084.pdf>. Internet. Accessed 26 January 2003.

General Accounting Office. Progress and Challenges to an Effective Defense-wide Information Assurance Program. Washington, D.C.: U.S. General Accounting Office, March 2001. Available from <http://www.gao.gov/new.items/d01307.pdf>. Internet. Accessed 26 January 2003.

Gilmore, Gerry J. "Strategic Influence Office 'Closed Down,' Says Rumsfeld." Armed Forces Information Service. 26 February 2002. Available from <http://www.defenselink.mil/news/ Feb2002/n02262002_200202263.html>. Internet. Accessed 2 February 2003.

Goodwin, Brent Stuart. “Don’t Techno for an Answer: The False Promise of Information Warfare.” Naval War College Review. (Spring 2000): 215-224.

Kahn, David, The Codebreakers. New York: Scribner, 1967, 1996.

Khalilzad, Zalmay M. and John B. White, eds. The Changing Role of Information Warfare. Santa Monica, CA: RAND, 1999.

Leonhard, Robert R. The Principles of War for the Information Age. Novato, CA: Presidio Press, 1998.

Patterson, LaWarren V. Information Operations and Asymmetric Warfare…Are We Ready? Strategy Research Project. Carlisle Barracks: U.S. Army War College, 9 April 2002.

Russell, Deborah and G.T. Gangemi Sr. Computer Security Basics, O'Reilly and Associates: Sebastopol, CA, 1991.

Schneier, Bruce. Secrets and Lies: Digital Security in a Network World. New York: John Wiley and Sons, 2000.

Seffers, George I. "Defense CIO Seeks a Promotion." Federal Computer Week. 11 December 2000. Available from <http://www.fcw.com/fcw/articles/2000/1211/news-cio-12-11-00.asp>. Internet. Accessed 16 February 2002.

Shelton, Henry H. Joint Vision 2020. Washington: Joint Staff, June 2000.

Snopes.com. "Baghdad Betty." Urban Legends Reference Pages. Available from <http://www.snopes.com/radiotv/radio/baghdad.htm>. Internet. Accessed 25 January 2003.

Stein, George P. Information Attack: Information Warfare in 2025. Maxwell Air Force Base: Air War College, August 1996. Available from <http://www.maxwell.af.mil/au/2025>. Internet. Accessed 14 Feb 2003.

The President’s Critical Infrastructure Protection Board. The National Strategy to Secure Cyberspace (Draft). September 2002. Available from <http://www.whitehouse.gov/pcipb/>. Internet. Accessed 3 November 2002.

Thompson, Mark. "America's Ultra-secret Weapon." Time. 19 January 2003. Available from <http://www.time.com/time/covers/1101030127/nmicro.html>. Internet. Accessed 2 February 2003.

Tomko, John S., Jr. Critical Infrastructure Protection. Strategy Research Project. Carlisle Barracks: U.S. Army War College, 9 April 2002.

U.S. Joint Chiefs of Staff. Department of Defense Dictionary of Military and Associated Terms. Joint Publication 1-02. Washington: Joint Staff, 12 April 2001.

U.S. Joint Chiefs of Staff. Joint Doctrine for Electronic Warfare. Joint Publication 3-51. Washington: Joint Staff, 7 April 2000.

U.S. Joint Chiefs of Staff. Joint Doctrine for Information Operations. Joint Publication 3-13. Washington: Joint Staff, 9 October 1998.

U.S. President. Executive Order. "Executive Order 12333–United States Intelligence Activities". Federal Register 46, (4 December 1981): 200.

United States Strategic Command. "Information Operations ". Available from <http://www.stratcom.af.mil/factsheetshtml/Information%20Operations.htm >. Internet. Accessed 2 Feb 2003.

United States Strategic Command. "Joint Task Force-Computer Network Defense". Available from <http://www.stratcom.af.mil/factsheetshtml/jtf-cno.htm>. Internet. Accessed 2 Feb 2003.

Widnall, Sheila E. and Ronald R. Fogleman. "Cornerstones of Information Warfare." 1995. Available from <http://www.af.mil/lib/corner.html>. Internet. Accessed 16 December 2002.